

his

(FILE 'USPAT' ENTERED AT 09:13:36 ON 18 DEC 1997)

L1 25 S (MACRO# AND (VIRUS? OR SCAN? OR INFECT?))/AB
L2 398 S (TEST? OR SCAN? OR DIAGNOS? OR ANALY? OR DEBUG?) (5A) M
ACR
L3 90 S L2 AND 395/CLAS
L4 22 S L3 AND 395/183####/CCLS
L5 1688 S (LOCAT? OR DETECT? OR SCAN?) (5A) (VIRUS?)
L6 38 S L5 AND 395/CLAS
L7 20 S L6 AND SIGNATURE#
L8 25 S L6 AND SCAN?
L9 16 S L8 AND L7
L10 744 S (TEST? OR DEBUG? OR SCAN? OR DIAGNOS? OR VIRUS? OR INFEC
T?)
L11 25 S L10 AND TEMPLATE (2A) (FILE#)
L12 0 S L11 AND VIRUS?
L13 3 S L11 AND 395/CLAS
L14 68123 S .DOT
L15 94 S L14 AND L10
L16 9 S L15 AND 395/CLAS
L17 249 S L5 AND L14
L18 0 S L17 AND 395/CLAS

=>

=> d 1-10

1. 5,696,822, Dec. 9, 1997, Polymorphic **virus** **detection** module; Carey Nachenberg, 380/4; 364/709.05; 380/1, 25; **395/183.01**, **183.09**, **183.14** [IMAGE AVAILABLE]
 2. 5,675,711, Oct. 7, 1997, Adaptive statistical regression and classification of data strings, with application to the generic **detection** of computer **viruses**; Jeffrey Owen Kephart, et al., **395/22**, **20**, **21** [IMAGE AVAILABLE]
 3. 5,657,473, Aug. 12, 1997, Method and apparatus for controlling access to and corruption of information in computer systems; Reginald Killeen, et al., 380/4; **395/182.21**, 711/163 [IMAGE AVAILABLE]
 4. 5,623,600, Apr. 22, 1997, **Virus** **detection** and removal apparatus for computer networks; Shuang Ji, et al., **395/187.01**, 364/286.4, DIG.1 [IMAGE AVAILABLE]
 5. 5,559,960, Sep. 24, 1996, Software anti-virus facility; Jonathan D. Lettvin, **395/186**, 380/4 [IMAGE AVAILABLE]
 6. 5,537,540, Jul. 16, 1996, Transparent, secure computer **virus** **detection** method and apparatus; Craig A. Miller, et al., **395/183.14**, **183.12**, **185.05** [IMAGE AVAILABLE]
 7. 5,511,163, Apr. 23, 1996, Network adaptor connected to a computer for virus **signature** recognition in all files on a network; Michael Lerche, et al., **395/183.04**, **183.15** [IMAGE AVAILABLE]
 8. 5,485,575, Jan. 16, 1996, Automatic analysis of a computer virus structure and means of attachment to its hosts; David M. Chess, et al., **395/183.14**, 380/4 [IMAGE AVAILABLE]
 9. 5,475,839, Dec. 12, 1995, Method and structure for securing access to a computer system; Bruce W. Watson, et al., **395/652**, 380/4; **395/186** [IMAGE AVAILABLE]
 10. 5,452,442, Sep. 19, 1995, Methods and apparatus for evaluating and extracting **signatures** of computer viruses and other undesirable software entities; Jeffrey O. Kephart, **395/183.14**, 380/4 [IMAGE AVAILABLE]
- => d 11-20
11. 5,440,723, Aug. 8, 1995, Automatic immune system for computers and computer networks; William C. Arnold, et al., **395/181**, **183.09**, **183.14** [IMAGE AVAILABLE]
 12. 5,421,006, May 30, 1995, Method and apparatus for assessing integrity of computer system software; David P. Jablon, et al., **395/183.12**, 380/4; **395/183.14** [IMAGE AVAILABLE]
 13. 5,414,833, May 9, 1995, Network security system and method using a parallel finite state machine adaptive active monitor and responder; Paul C. Hershey, et al., **395/187.01**, 380/4, 49 [IMAGE AVAILABLE]
 14. 5,408,642, Apr. 18, 1995, Method for recovery of a computer program infected by a computer virus; Omri Mann, **395/183.14**, 371/30, 67.1

[IMAGE AVAILABLE]

15. 5,398,196, Mar. 14, 1995, Method and apparatus for **detection** of computer **viruses**; David A. Chambers, 364/580, 550, 578, 579; **395/500** [IMAGE AVAILABLE]
16. 5,361,359, Nov. 1, 1994, System and method for controlling the use of a computer; Homayoon Tajalli, et al., **395/186**; 340/825.31; 364/918.7, DIG.2 [IMAGE AVAILABLE]
17. 5,349,655, Sep. 20, 1994, Method for recovery of a computer program infected by a computer virus; Omri Mann, **395/182.04**; 380/4, 25 [IMAGE AVAILABLE]
18. 5,319,776, Jun. 7, 1994, In transit **detection** of computer **virus** with safeguard; John K. Hile, et al., **395/186**; 371/67.1; 380/4 [IMAGE AVAILABLE]
19. 5,274,819, Dec. 28, 1993, Management system for memory resident computer programs; Christopher Blomfield-Brown, **395/670**; 364/228.1, 231, 234, 234.3, 236.2, 236.8, 237.2, 237.3, 239, 239.8, 246.8, 247, 247.4, 248.1, 254, 254.3, 280, 280.9, 284.3, 286, 286.1, 286.2, 286.3, DIG.1 [IMAGE AVAILABLE]
20. 5,121,345, Jun. 9, 1992, System and method for protecting integrity of computer data and software; Stephen A. Lentz, 364/550, 231, 236.2, 238.5, 240, 244, 244.6, 248.1, 259, 259.9, 262.4, 262.9, 280, 280.2, 285, 285.4, 286.4, 286.5, DIG.1; 380/4; **395/186**, **652** [IMAGE AVAILABLE]
=>

d 1-

1. 5,696,822, Dec. 9, 1997, Polymorphic **virus** **detection** module; Carey Nachenberg, 380/4; 364/709.05; 380/1, 25; **395/183.01**, **183.09**, **183.14** [IMAGE AVAILABLE]
2. 5,675,711, Oct. 7, 1997, Adaptive statistical regression and classification of data strings, with application to the generic **detection** of computer **viruses**; Jeffrey Owen Kephart, et al., **395/22**, **20**, **21** [IMAGE AVAILABLE]
3. 5,623,600, Apr. 22, 1997, **Virus** **detection** and removal apparatus for computer networks; Shuang Ji, et al., **395/187.01**, 364/286.4, DIG.1 [IMAGE AVAILABLE]
4. 5,559,960, Sep. 24, 1996, Software anti-virus facility; Jonathan D. Lettvin, **395/186**, 380/4 [IMAGE AVAILABLE]
5. 5,537,540, Jul. 16, 1996, Transparent, secure computer **virus** **detection** method and apparatus; Craig A. Miller, et al., **395/183.14**, **183.12**, **185.05** [IMAGE AVAILABLE]
6. 5,511,163, Apr. 23, 1996, Network adaptor connected to a computer for virus **signature** recognition in all files on a network; Michael Lerche, et al., **395/183.04**, **183.15** [IMAGE AVAILABLE]
7. 5,485,575, Jan. 16, 1996, Automatic analysis of a computer virus structure and means of attachment to its hosts; David M. Chess, et al., **395/183.14**, 380/4 [IMAGE AVAILABLE]
8. 5,475,839, Dec. 12, 1995, Method and structure for securing access to a computer system; Bruce W. Watson, et al., **395/652**, 380/4; **395/186** [IMAGE AVAILABLE]
9. 5,452,442, Sep. 19, 1995, Methods and apparatus for evaluating and extracting **signatures** of computer viruses and other undesirable software entities; Jeffrey O. Kephart, **395/183.14**, 380/4 [IMAGE AVAILABLE]
10. 5,440,723, Aug. 8, 1995, Automatic immune system for computers and computer networks; William C. Arnold, et al., **395/181**, **183.09**, **183.14** [IMAGE AVAILABLE]
11. 5,414,833, May 9, 1995, Network security system and method using a parallel finite state machine adaptive active monitor and responder; Paul C. Hershey, et al., **395/187.01**, 380/4, 49 [IMAGE AVAILABLE]
12. 5,398,196, Mar. 14, 1995, Method and apparatus for **detection** of computer **viruses**; David A. Chambers, 364/580, 550, 578, 579; **395/500** [IMAGE AVAILABLE]
13. 5,361,359, Nov. 1, 1994, System and method for controlling the use of a computer; Homayoon Tajalli, et al., **395/186**, 340/825.31; 364/918.7, DIG.2 [IMAGE AVAILABLE]
14. 5,319,776, Jun. 7, 1994, In transit **detection** of computer **virus** with safeguard; John K. Hile, et al., **395/186**, 371/67.1; 380/4 [IMAGE AVAILABLE]

15. 5,274,819, Dec. 28, 1993, Management system for memory resident computer programs; Christopher Blomfield-Brown, **395/670**; 364/228.1, 231, 234, 234.3, 236.2, 236.8, 237.2, 237.3, 239, 239.8, 246.8, 247, 247.4, 248.1, 254, 254.3, 280, 280.9, 284.3, 286, 286.1, 286.2, 286.3, DIG.1 [IMAGE AVAILABLE]

16. 5,121,345, Jun. 9, 1992, System and method for protecting integrity of computer data and software; Stephen A. Lentz, 364/550, 231, 236.2, 238.5, 240, 244, 244.6, 248.1, 259, 259.9, 262.4, 262.9, 280, 280.2, 285, 285.4, 286.4, 286.5, DIG.1; 380/4; **395/186**, **652** [IMAGE AVAILABLE]
=>

APPLICATION-DATA:

PUB-NO	APPL-SCRIPTOR	APPL-NO	APPL-DATE
DE69315690E	N/A	1993DE-0615690	April 28, 1993
DE69315690E	N/A	1993EP-0909808	April 28, 1993
DE69315690E	N/A	1993WO-DK00140	April 28, 1993
DE69315690E	Based on	EP 638184	N/A
DE69315690E	Based on	WO 9322723	N/A
WO 9322723A1	N/A	1993WO-DK00140	April 28, 1993
DK 9200550A	N/A	1992DK-0000550	April 28, 1992
DK 9201264A	N/A	1992DK-0001264	October 15, 1992
AU 9340600A	N/A	1993AU-0040600	April 28, 1993
AU 9340600A	Based on	WO 9322723	N/A
EP 638184A1	N/A	1993EP-0909808	April 28, 1993
EP 638184A1	N/A	1993WO-DK00140	April 28, 1993
EP 638184A1	Based on	WO 9322723	N/A
DK 170490B	N/A	1992DK-0001264	October 15, 1992
DK 170490B	Previous Publ.	DK 9201264	N/A
DK 170544B	N/A	1992DK-0000550	April 28, 1992
DK 170544B	Previous Publ.	DK 9200550	N/A
US 5511163A	N/A	1994US-0325466	December 19, 1994
EP 638184B1	N/A	1993EP-0909808	April 28, 1993
EP 638184B1	N/A	1993WO-DK00140	April 28, 1993
EP 638184B1	Based on	WO 9322723	N/A

IPC: G06F001/00; G06F011/00 ; G06F011/30 ; G06F012/14 ; H04L012/26 ;
H04L029/14

ABSTRACTED-PUB-NO:EP 638184B

BASIC-ABSTRACT:The data processing system includes a number of computers (2) interconnect ed through a local network (1) and also to a network adapter (7). The network adapter has a computer (8) connected to it. This computer can monitor all the traffic on the network. The computer monitors file packets transmitted and can reassemble substantially all files on the network. The recreated files can be scanned for virus infection. If a virus is found, a vaccine program can be transmitted to the transmitter and receiver of the infected files. Further a neural network can monitor traffic patterns and raise a warning if these alter substantially.
ADVANTAGE - Detects virus infection on local network, eg ring network earlier and reduces down-time for repair of system.

ABSTRACTED-PUB-NO:US 5511163A

EQUIVALENT-ABSTRACT:The data processing system includes a number of computers (2) interconnect ed through a local network (1) and also to a network adapter (7). The network adapter has a computer (8) connected to it. This computer can monitor all the traffic on the network. The computer monitors file packets transmitted and can reassemble substantially all files on the network. The recreated files can be scanned for virus infection. If a virus is found, a vaccine program can be transmitted to the transmitter and receiver of the infected files. Further a neural network can monitor traffic patterns and raise a warning if these alter substantially.
ADVANTAGE - Detects virus infection on local network, eg ring network earlier and reduces down-time for repair of system. A data processing system comprising a plurality of computers interconnecte d through a local network in the form of a ring network, said network being connected to a network adaptor which is able to receive information on the network, characterized in that the network adaptor (7) is connected to a computer (8), which together with the adaptor (7) can perform an assembling and scanning of substantially all files on the network (1) and carry out a recognition of virus signatures, if any, in the files, the computer (8) being adapted to provide information on the place of origin of infected data, if any, as well as on the position to which said infected data has been transmitted, and comprising a neural network having program means for recognizing the usual interchange of data on the local network (1) and for activating an alarm if an unusual interchange of data resembling a virus, such as an unknown virus signature, is recognized.

CHOSEN-DRAWING:Dwg.1/7 Dwg.1 Dwg.1/7